Patent
Orrick Docket No. 16057.4003

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

ISHIKAWA, Mark M.

Serial No.: 09/821,565

Filed: March 29, 2001

For: SYSTEM, METHOD AND APPARATUS FOR DETECTING, IDENTIFYING AND RESPONDING TO FRAUDULENT REQUESTS ON A NETWORK

Group Art Unit: 2134

Examiner: Tongoc Tran

AMENDMENT AND RESPONSE

Mail Stop AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Office Action dated February 28, 2006, please enter the following amendments.

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that I have reasonable basis to expect that that this paper or fee (along with any referred to as being attached or enclosed) was transmitted electronically to Mail Stop Amendment, Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Dated: May 23, 2006

Karen L. Johnson
Karen L. Johnson

IN THE CLAIMS

Please amend the following claims:

1 - 39. (Canceled)

40. (Currently Amended) A system for identifying and diverting problematic information packets transmitted from a first network device to a second network device, comprising:

a switching system that provides a network address of the second network device to the first network device, said switching system receiving ~~the~~ information packets from the first network device and directing the information packets to the second network device;

a route arbitration system that monitors the information packets received by said switching system, said route arbitration system determining whether the information packets comprise abnormal network activity in accordance with a first predetermined criteria and, if said route arbitration system determines that the information packets comprise abnormal network activity, identifying the information packets as being abnormal information packets; and

a traffic analysis system that monitors the abnormal information packets identified by said route arbitration system, said traffic analysis system determining whether the abnormal information packets are problematic in accordance with a second predetermined criteria and, if said traffic analysis system determines that the abnormal information packets are problematic, identifying the abnormal information packets as being the problematic information packets and inhibiting said switching system from providing the network address of the second network device to the first network device,

wherein said switching system, when inhibited, renders the second network device unreachable and prevents the first network device from transmitting the problematic information packets to said switching system.

41. (Previously Presented) The system of claim 40, wherein said switching system includes a routing system.

42. (Previously Presented) The system of claim 40, wherein said route arbitration system is at least partially incorporated into said switching system.

43. (Previously Presented) The system of claim 40, wherein said route arbitration system communicates with said switching system via at least one communication link selected from the group consisting of a remote monitoring network probe, a switching device, and an Ethernet probe.

44. (Previously Presented) The system of claim 40, wherein said route arbitration system monitors a volume of the information packets.

45. (Previously Presented) The system of claim 44, wherein said route arbitration system determines that the information packets comprise said abnormal network activity when the volume of the information packets is greater than a preselected volume threshold level.

46. (Previously Presented) The system of claim 40, wherein said route arbitration system, upon determining that the information packets no longer comprise said abnormal network activity, enables said switching system to again provide the network address of the second network device to the first network device and receive the information packets from the first network device.

47. (Previously Presented) The system of claim 40, wherein said traffic analysis system is at least partially incorporated into said switching system.

48. (Previously Presented) The system of claim 40, wherein said traffic analysis system monitors a volume of the abnormal information packets.

49. (Previously Presented) The system of claim 48, wherein said traffic analysis system determines that the abnormal information packets are problematic when the volume of the abnormal information packets is greater than a preselected volume threshold level.

50. (Previously Presented) The system of claim 48, wherein said traffic analysis system determines that the abnormal information packets are problematic when the volume of the abnormal information packets does not decrease during a preselected time interval.

51. (Previously Presented) The system of claim 40, wherein said traffic analysis system instructs said switching system to redirect the information packets to a null network device having a null address, said null network device receiving the information packets and providing no response to the first network device.

52. (Currently Amended) The system of claim 51 ~~52~~, wherein said traffic analysis system instructs said switching system to provide said null address to the first network device such that the first network device transmits the problematic information packets to said null network device.

53. (Previously Presented) The system of claim 52, wherein said null network device is provided by at least one of said route arbitration system and said traffic analysis system.

54. (Previously Presented) The system of claim 40, further comprising a firewall system that identifies suspect information packets received from the first network device, said switching system directing the information packets to the second network device via said firewall system.

55. (Previously Presented) The system of claim 54, wherein said traffic analysis system determines whether the suspect information packets are problematic and, if said traffic analysis system determines that the suspect information packets are problematic, inhibits said switching system from providing the network address of the second network device to the first network device.

56. (Currently Amended) A system for identifying and diverting problematic information packets transmitted from a first network device to a second network device, comprising:

a switching system that provides a network address to the first network device, said switching system receiving ~~the~~ information packets from the first network device and directing the information packets to the second network device; and

an activity monitoring system that monitors the information packets received by said switching system, said activity monitoring system ~~route arbitration system~~ determining whether the information packets are problematic in accordance with at least one predetermined criteria and, if said activity monitoring system determines that the information packets are problematic, identifying the information packets as being the problematic information packets and inhibiting said switching system from providing the network address of the second network device to the first network device,

wherein said switching system, when inhibited, renders the second network device unreachable and prevents the first network device from transmitting the problematic information packets to said switching system.

57. (Previously Presented) The system of claim 56, wherein said activity monitoring system monitors a volume of the information packets and determines that the information packets are problematic when the volume of the information packets is greater than a preselected volume threshold level.

58. (Previously Presented) The system of claim 57, wherein said activity monitoring system monitors a volume of the information packets that exceed said preselected volume threshold level and determines that the information packets are problematic when the volume of the information packets exceeding said preselected volume threshold level does not decrease during a preselected time interval.

59. (Previously Presented) The system of claim 56, wherein said activity monitoring system includes:

a route arbitration system that monitors the information packets received by said switching system, said route arbitration system determining whether the information packets comprise abnormal network activity in accordance with a first predetermined criteria and, if said route arbitration system determines that the information packets comprise abnormal network activity, identifying the information packets as being abnormal information packets; and

a traffic analysis system that monitors the abnormal information packets identified by said route arbitration system, said traffic analysis system determining whether the abnormal information packets comprise the problematic information packets in accordance with a second predetermined criteria and, if said traffic analysis system determines that the abnormal information packets comprise the problematic information packets, inhibiting said switching system from providing the network address of the second network device to the first network device.

60. (Currently Amended) A system for identifying and diverting problematic information packets received from an external network device, comprising:

a protected network device having a network address;

a switching system that provides said network address to the external network device, said switching system receiving ~~the~~ information packets from the external network device and directing the information packets to said protected network device;

a route arbitration system that monitors the information packets received by said switching system, said route arbitration system determining whether the information packets comprise abnormal network activity in accordance with a first predetermined criteria and, if said route arbitration system determines that the information packets comprise abnormal network activity, identifying the information packets as being abnormal information packets; and

a traffic analysis system that monitors the abnormal information packets identified by said route arbitration system, said traffic analysis system determining whether the abnormal information packets are problematic in accordance with a second predetermined criteria and, if said traffic analysis system determines that the abnormal information packets are problematic, identifying the abnormal information packets as being the problematic information packets and inhibiting said switching system from providing the network address of said protected network device to the external network device,

wherein said switching system, when inhibited, renders said protected network device unreachable and prevents the external network device from transmitting the problematic information packets to said switching system.

61. (Previously Presented) The system of claim 60, wherein said protected network device comprises at least one network device selected from the group consisting of a server system, a computer system, a provider computer system, a user computer system, a router system, an edge router system, a core router system, and a firewall.

62. (Previously Presented) The system of claim 60, further comprising a communication system, said switching system communicating with the external network device via said communication system.

63. (Previously Presented) The system of claim 62, wherein said communication system comprises a communication link selected from the group consisting of a local area network, a wired communication network, a wireless communication network, a wide area network, a public communication network, and the Internet.

64. (Previously Presented) The system of claim 60, wherein said route arbitration system monitors a volume of the information packets and determines that the information packets comprise said abnormal network activity when the volume of the information packets is greater than a preselected volume threshold level.

65. (Previously Presented) The system of claim 60, wherein said route arbitration system, upon determining that the information packets no longer comprise said abnormal network activity, enables said switching system to again provide the network address of the protected network device to the external network device and receive the information packets from the external network device.

66. (Previously Presented) The system of claim 60, wherein said traffic analysis system monitors a volume of the abnormal information packets and determines that the abnormal information packets are problematic when the volume of the abnormal information packets is greater than a preselected volume threshold level.

67. (Previously Presented) The system of claim 60, wherein said traffic analysis system monitors a volume of the abnormal information packets and determines that the abnormal information packets are problematic when the volume of the abnormal information packets does not decrease during a preselected time interval.

68. (Previously Presented) The system of claim 60, wherein said traffic analysis system instructs said switching system to redirect the information packets to a null network device having a null address, said null network device receiving the information packets and providing no response to the external network device.

69. (Previously Presented) The system of claim 60, further comprising a firewall system that identifies suspect information packets received from the external network device, said switching system directing the information packets to the protected network device via said firewall system, said traffic analysis system determining whether the suspect information packets are problematic and, if said traffic analysis system determines that the suspect information packets are problematic, inhibiting said switching system from providing the network address of the protected network device to the external network device.

70. (Previously Presented) The system of claim 60, wherein said traffic analysis system instructs said switching system to redirect the information packets to a traffic analysis device, said traffic analysis device receiving and analyzing the information packets.

71. (Currently Amended) A method for identifying and diverting problematic information packets transmitted from a first network device to a second network device, comprising:

providing a network address of the second network device to the first network device via a switching system receiving ~~the~~ information packets from the first network device and directing the information packets to said second network device;

monitoring the information packets received from the first network device;

determining whether the information packets comprise abnormal network activity in accordance with a first predetermined criteria;

if the information packets are determined to comprise abnormal network activity, identifying the information packets as being abnormal information packets;

monitoring the abnormal information packets;

determining whether the abnormal information packets are problematic in accordance with a second predetermined criteria; and

if the abnormal information packets are determined to be problematic,

identifying the abnormal information packets as being the problematic information packets; and

inhibiting said switching system from providing the network address of said second network device to the first network device,

wherein said switching system, when inhibited, renders the second network device unreachable and prevents the first network device from transmitting the problematic information packets to said switching system.

72. (Previously Presented) The method of claim 71, wherein said monitoring the information packets includes monitoring a volume of the information packets and wherein said determining whether the information packets comprise said abnormal network activity includes determining that the information packets comprise said abnormal network activity when the volume of the information packets is greater than a preselected volume threshold level.

73. (Previously Presented) The method of claim 71, wherein said monitoring the abnormal information packets includes monitoring a volume of the abnormal information packets and wherein said determining whether the abnormal information packets are problematic includes determining that the abnormal information packets are problematic when the volume of the abnormal information packets does not decrease during a preselected time interval.

74. (Previously Presented) The method of claim 71, further comprising determining that the information packets no longer comprise said abnormal network activity and enabling said switching system to again provide the network address of the second network device to the first network device and receive the information packets from the first network device.

75. (Previously Presented) The method of claim 71, wherein said inhibiting said switching system includes redirecting the information packets to a null network device having a null address, said null network device receiving the information packets and providing no response to the first network device.

76. (Previously Presented) The method of claim 75, wherein said redirecting the information packets includes instructing said switching system to provide said null address to the first network device such that the first network device transmits the problematic information packets to said null network device.

77. (Currently Amended) A method for identifying and diverting problematic information packets transmitted from a first network device to a second network device, comprising:

providing a network address of the second network device to the first network device via a switching system receiving ~~the~~ information packets from the first network device and directing the information packets to said second network device;

monitoring the information packets received from the first network device;

determining whether the information packets are problematic in accordance with at least one predetermined criteria; and

if the information packets are determined to be problematic,

identifying the information packets as being the problematic information packets; and

inhibiting said switching system from providing the network address of said second network device to the first network device,

wherein said switching system, when inhibited, renders the second network device unreachable and prevents the first network device from transmitting the problematic information packets to said switching system.

78. (Previously Presented) The method of claim 77, wherein said determining whether the information packets are problematic includes:

determining whether the information packets comprise abnormal network activity in accordance with a first predetermined criteria;

if the information packets are determined to comprise abnormal network activity, identifying the information packets as being abnormal information packets;

monitoring the abnormal information packets; and

determining whether the abnormal information packets are problematic in accordance with a second predetermined criteria.

Please add the following new claims:

79. (New) A method for identifying an efficient communication path in a network coupling a first network device and a second network device, comprising:

analyzing a network load on the network;

defining at least one known communication path between the first network device and the second network device, said at least one known communication path including a plurality of independent path segments coupled via communication links;

determining an availability of each of said path segments to identify one or more available path segments for said at least one known communication path;

determining an availability of each of said communication links to identify one or more available communication links for said at least one known communication path;

combining at least one of said available path segments and at least one of said available communication links to form the efficient communication path such that an amount of time to exchange network traffic between the first network device and the second network device is minimized; and

routing the network traffic between the first network device and the second network device via the efficient communication path.

80. (New) The method of claim 79, wherein said combining said at least one of said available path segments and said at least one of said available communication links includes transmitting a sample packet from the first network device to the second network device and measuring a time interval for the sample packet to return to the first network device.

REMARKS

Reconsideration of the objection and the rejections set forth in the Office Action dated February 28, 2006, is respectfully requested. The Examiner rejected claims 40-78. Applicant has amended claims 40, 52, 56, 60, 71, and 77 and added new claims 79 and 80, which are based upon original claims 14 and 15 and find support, for example, on page 13, line 23 – page 14, line 8 of the original specification as filed. Accordingly, claims 40-80 remain pending in the application. No new matter has been added by these amendments as can be confirmed by the Examiner.

A. The Claim Amendments Are Not Made for Substantial Reasons Related to Patentability

In the Office Action, the Examiner objected to claim 52, noting a typographical error in the claim, and rejected claim 56 under 35 U.S.C. § 112, ¶ 2 for lacking sufficient antecedent basis for the claim term "said arbitration system." Applicant appreciates the Examiner's careful examination of the present application and has made appropriate amendments to the claims 52 and 56. Applicant likewise has amended claims 40, 56, 60, 71, and 77 to correct other typographical errors. These claim amendments were made merely to correct minor typographical errors and to more clearly recite the claimed subject matter. Therefore, the claim amendments have not been made for substantial reasons related to patentability.

B. The Prior Art Does Not Disclose or Suggest a Switching System that Provides a Network Address of a Protected Network Device to Another Network Device and, When Information Packets Received from the Other Network Device are Identified as Problematic, is Inhibited from Providing the Network Address to the Other Network Device, Rendering the Protected Network Device Unreachable and Preventing the Other Network Device from Transmitting the Problematic Information Packets to the Switching System as Recited in Claims 40-78.

In the Office Action, the Examiner rejected claims 40-44, 46-48, 54-56, 59, 60-63, 69-71, 77, and 78, including independent claims 40, 56, 60, 71, and 77, under 35

U.S.C. § 102(e) as allegedly being anticipated by Shanklin et al., United States Patent No. 6,578,147, and asserted that each of the other pending claims are rendered obvious under 35 U.S.C. § 103(a) by Shanklin et al. in view of either Schuba, United States Patent No. 6,725,378, Putzolu et al., United States Patent No. 6,587,432, or Gibbings, United States Patent No. 6,885,675. Applicant respectfully submits, however that, by failing to disclose each and every element of independent claims 40, 56, 60, 71, and 77, neither Shanklin et al., Schuba, Putzolu et al., nor Gibbings anticipates or renders obvious claims 40, 56, 60, 71, and 77. Therefore, it is submitted that independent claims 40, 56, 60, 71, and 77, as well as claims 41-55, 57-59, 61-70, 72-76, and 78 that depend respectively thereon, are in condition for allowance.

A switching system is set forth in each independent claim 40, 56, 60, 71, and 77. A typical recitation of the switching system is set forth in claim 40, as amended, which recites:

> "a switching system that provides a network address of the second network device to the first network device, said switching system receiving information packets from the first network device and directing the information packets to the second network device;"
>
> "a traffic analysis system ... determining whether the abnormal information packets are problematic in accordance with a second predetermined criteria and, if said traffic analysis system determines that the abnormal information packets are problematic, ... inhibiting said switching system from providing the network address of the second network device to the first network device,"
>
> "wherein said switching system, when inhibited, renders the second network device unreachable and prevents the first network device from transmitting the problematic information packets to said switching system."

Therefore, claimed switching system provides a network address of a protected network device to another network device and receives information packets from the other network device, directing the received information packets to the protected device during normal operation. If one or more of the information packets received from the other network device are identified as being problematic information packets, the switching system, as claimed, is inhibited from providing the network address to the other network device. Because of this inhibition, the switching system prevents the other network device from transmitting the problematic information packets to the switching system such that the protected network device is rendered unreachable by the other network device.

Shanklin et al. disclose a protected local computer network 10 that exchanges data packets with an external network via a router 12 and that is protected by an intrusion detection system (IDS) sensor 11. See Shanklin et al. at Fig. 1; col. 3, lines 11-18. In contrast to the claimed switching system, Shanklin et al. do not teach that the router 12 provides a network address of the local computer network 10 to the external network. The intrusion detection system sensor 11 likewise is not disclosed as being adapted to inhibit the router 12 from providing the network address of the local computer network 10 to the external network. Further, Shanklin et al. do not teach that, by inhibiting the router 12 from providing the network address to the external network, the local computer network 10 can be rendered unreachable by the external network or the external network can be prevented from transmitting problematic information packets to the local computer network 10.

As readily admitted by the Examiner, Shanklin et al. at best make passing mention of terminating a connection when an intrusion is detected. This vague reference appears at col. 3, lines 62-65 and states that "sensor 11 may have appropriate functionality so that if it detects an intrusion, it can take appropriate action, such as terminating the connection." The Examiner however relies solely upon this vague reference, asserting that "even if Shanklin's system teaches one of the appropriate action [sic] is terminating the connection would still meet the claimed limitation of inhibiting or rendering the second networks [sic, "second network device"] unreachable and prevents the first network device from transmitting the problematic information packets to said switching system as claimed in independent claims."

At least one recited element of claims 40, 56, 60, 71, and 77 therefore is totally missing from Shanklin et al. In accordance with M.P.E.P. § 2131, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987) (emphasis added). The disclosure of a claim element in a prior art reference, when relied upon to negate patentability, must also be clear and unambiguous. Further, "[t]he identical invention must be shown in as complete detail as contained in the...claim." *Richardson v. Suzuki Motor Corp.*, 868 F.2d 1226, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989). Furthermore, and uniquely important in this case is the requirement that the elements relied on in the prior art reference must be arranged as required by the claim. See *In re Bonds*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990).

Applicant therefore submits that independent claims 40, 56, 60, 71, and 77, as well as claims 41-55, 57-59, 61-70, 72-76, and 78 that depend respectively thereon, are not anticipated by Shanklin et al. and are in condition for allowance.

C. No Motivation Exists to Modify the Teachings of Prior Art in a Manner that Precludes the Patentability of Claims 40-78 Under 35 U.S.C. § 103.

In accordance with M.P.E.P. § 2142, the Examiner bears the initial burden of establishing a *prima facie* case of obviousness. "To establish a *prima facie* case of obviousness, three basic criteria must be met." (M.P.E.P. § 2143.) First, some suggestion or motivation in the prior art references or in the knowledge of one of ordinary skill in the relevant art must exist to modify or combine the references. Second, if the references are combined, a reasonable expectation of success must be shown. Then, finally, all of the claim limitations must be taught or suggested by one reference or a combination of references. To establish a *prima facie* case of obviousness based on a single reference that does not teach all the elements of a claim, the Examiner must provide a rationale for modifying the teachings of the reference. See *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000), *citing*, *B.F. Goodrich Co. v. Aircraft Breaking Sys. Corp.*, 72 F.3d 1577, 1582, 37 U.S.P.Q.2d 1314, 1318 (Fed. Cir. 1996).

Here, the Examiner asserts that dependent claims 46, 65, and 74 are rendered obvious by Shanklin et al. in view of Schuba, that dependent claims 45, 49, 50, 57, 58, 64, 66, 67, 72, and 73 are rendered obvious by Shanklin et al. in view of Putzolu et al., and that dependent claims 51-53, 75 and 76 are rendered obvious by Shanklin et al. in view of Gibbings. As discussed above, however, at least one recited element of claims 40-78 is totally missing from Shanklin et al. Further, the Examiner does not assert that any suggestion or motivation in the prior art references or in the knowledge of one of ordinary skill in the relevant art exists to modify Shanklin et al. or to combine Shanklin et al. with Schuba, Putzolu et al., or Gibbings in a manner that renders claims 40-78 obvious. The Examiner therefore has not established a *prima facie* case under 35 U.S.C. § 103 because, as shown above, all of the elements of the pending claims are not found in the cited references.

According, it is submitted that the cited prior art does not anticipate or render obvious independent claims 40, 56, 60, 71, and 77. Applicant therefore submits that claims 40, 56, 60, 71, and 77, as well as claims 41-55, 57-59, 61-70, 72-76, and 78 that depend respectively thereon, are in condition for allowance.

D. The Prior Art Does Not Disclose or Suggest a Method for Identifying an Efficient Communication Path in a Network Coupling a First Network Device and a Second Network Device as Recited in New Claims 79-80.

In manner discussed above with reference to claim 40-78, neither Shanklin et al., Schuba, Putzolu et al., nor Gibbings anticipates or renders obvious new claims 79-80. Therefore, it is submitted that claims 79-80, are in condition for allowance.

In contrast to the systems and method recited in new claims 79-80, none of the cited prior art references, either individually or in combination, disclose or suggest a method whereby at least one available path segment and at least one available communication link are combined to form an efficient communication path such that an amount of time to exchange network traffic between a first network device and a second network device is minimized. At least one recited element of new claims 79-80, therefore, is totally missing from Shanklin et al., Schuba, Putzolu et al., and Gibbings. Accordingly, since the cited prior art fails to disclose each and every element of claims 79-80, new claims 79-80 are not anticipated. Applicant therefore submits that new claims 79-80 are in condition for allowance.

For at least the reasons set forth above, it is submitted that claims 40-80 are in condition for allowance. A Notice of Allowance is earnestly solicited. The Examiner is encouraged to contact the undersigned at (949) 567-6700 if there is any way to expedite the prosecution of the present application.

Respectfully submitted,
Orrick, Herrington & Sutcliffe LLP

Dated: May 23, 2006

By: Davin M. Stockwell
Davin M. Stockwell
Reg. No. 41,334
Attorneys for Applicants

Orrick, Herrington & Sutcliffe LLP
4 Park Plaza, Suite 1600
Irvine, California 92614-2558
Telephone: (949) 567-6700
Facsimile: (949) 567-6710